• "Uniquely corresponding." See Appendix A. Most fingerprints and digital signatures could conceivably correspond to multiple electronic records. However, the likelihood of finding a corresponding electronic record other than the one of interest, given a uniform probability of obtaining all possible fingerprints or digital signatures from a given record, is usually vanishingly small. The likelihood of finding a second match that could be mistaken for the electronic record of interest is so small, in most cryptographic applications, as to be considered impossible. Embodiments are certainly possible, however, in which an electronic record may be considered to uniquely correspond to a fingerprint or digital signature with a higher probability of a false match.

• "Virtual signature printing," "Virtual signature printer." Authenticating an electronic record such as a word processor document by "printing" the document using a printer driver that does not actually produce printed output, at least not as its main purpose. Instead, such a printer driver according to various aspects of the inventions creates another file that includes, or references, indicia of the user's digital signature authentication of the electronic record. See Appendix AD-1.

APPENDICES A - AL

See following sheets.

CLAIM

What is claimed is:

1. A method for authenticating a digital signature key, the method comprising:

(a) preparing a record including an integrated combination of (1) indicia uniquely corresponding to the key, and (2) indicia of a covenant not to repudiate any digital signature made with the key except under specified conditions; and

(b) having an owner of the key perform a legally accepted execution of the record;

whereby the owner enters into a covenant with any bearer of the record not to repudiate any digital signature made with the key except under the specified conditions.